

Zes afwegingen voor Identity & Access Management

Bespreek één werkproces of applicatie. Leg per overweging vast welk besluit nog nodig is en welk bewijs laat zien dat de toegangsafspraken werkt.

Werkproces of applicatie

Datum overleg

01 Sluiten rollen aan op taken, risico's en beslisbevoegdheden?

Onderbouw welke handelingen bij een rol horen en welke combinaties ongewenste bevoegdheden opleveren. Maak onderscheid tussen organisatieonderdelen, functies en applicatierechten. Bepaal wie een rol mag wijzigen en hoe uitzonderingen tijdelijk, traceerbaar en herroepbaar blijven.

☐ Besproken

Notitie of besluit

02 Welke bron bepaalt de identiteit en welke gebeurtenis wijzigt de toegang?

Leg vast hoe instroom, functiewijziging, uitdiensttreding en het einde van externe inzet worden signaleerd. Bepaal de toegestane verwerkingstijd per gebeurtenis. Toets hoe ontbrekende of conflicterende brongegevens worden afgehandeld zonder dat rechten blijven bestaan zonder eigenaar.

☐ Besproken

Notitie of besluit

03 Welke toegang vraagt om extra waarborgen?

Onderscheid normale gebruikersrechten, beheerdersrechten, noodtoegang en accounts voor systeemkoppelingen. Weeg authenticatie, toegangsduur en benodigde goedkeuring af tegen het risico. Leg vast hoe vertrouwelijke aanmeldgegevens worden beheerd en hoe gebruik achteraf kan worden verantwoord.

☐ Besproken

Notitie of besluit

Van beoordeling naar vervolgactie

Identity & Access Management | Overwegingen 4 tot en met 6

04 Wie beoordeelt bestaande rechten op inhoudelijke noodzaak?

Bepaal welke proceseigenaar kan vaststellen of toegang nog nodig is. Zorg dat de beoordeling begrijpelijke handelingen toont in plaats van alleen technische codes. Leg vast hoe intrekking wordt uitgevoerd, hoe uitzonderingen worden opgevolgd en hoe afronding aantoonbaar wordt gemaakt.

☐ Besproken Notitie of besluit

05 Hoe voorkomen we inconsistentie tussen applicaties en koppelingen?

Onderzoek waar rechten centraal worden beheerd en waar lokale uitzonderingen ontstaan. Toets of intrekken van een account ook sessies, gekoppelde toegang en afgeleide rechten raakt. Spreek af hoe verschillen worden gesignaleerd en welke partij herstel over de hele keten coördineert.

☐ Besproken Notitie of besluit

06 Hoe toetsen we zowel ongewenste toegang als werkbaarheid?

Test toegestane én verboden handelingen met representatieve rollen, inclusief functiewissels en tijdelijke toegang. Beoordeel of controles het werk uitvoerbaar houden. Leg vast wie afwijkingen oplost, welke bevindingen ingebruikname blokkeren en wie de inrichting na wijzigingen opnieuw controleert.

☐ Besproken Notitie of besluit

Onze eerste vervolgstap

Actie en beoogd resultaat

Eigenaar

Afgesproken datum